

We claim:

①. Rs 4/- (original) A packet switching controller comprising:

146

an input for receiving a packet;
166
a policing element for classifying the packet
into a plurality of policeable groups,

wherein the packet is compared against one or more bandwidth contracts defined for the policeable groups to produce one or more policing results.

10

2.¹⁵⁷ (original) The packet switching controller of claim 1 wherein the policing element includes a policing database, a first policeable group identifier is applied to the policing database to retrieve first policing data and a second policeable group identifier, the first policing data is applied to produce a first policing result, the second policeable group identifier is applied to the policing database to retrieve second policing data, and the second policing data is applied to produce a second policing result.

15

20

3. (original) The packet switching controller of claim 1 further comprising a disposition engine for making a disposition decision for the packet, wherein the policing results include one or more disposition recommendations, and the disposition engine uses the policing results and at least one other disposition recommendation to make the disposition decision for the packet.

25

30

4. (original) The packet switching controller of claim 1 wherein the policing results are combined into a single result by taking a worst case policing result.

5. ^{§ 4} (original) A method of processing a packet using a policing element, the method comprising the steps of:

receiving the packet;

5 classifying the packet into a plurality of policeable groups; and

comparing the packet against one or more bandwidth contracts defined for the policeable groups to produce one or more policing results.

10

6. ^{§ 7} (original) The method of processing a packet of claim 5 wherein the policing element includes a policing database, and the method further comprises the steps of:

applying a first policeable group identifier to the policing database to retrieve first policing data and a second policeable group identifier;

15 producing a first policing result using the first policing data;

applying the second policeable group identifier to the policing database to retrieve second policing data; and

producing a second policing result using the second policing data.

25

7. ^{§ 4} (original) The method of processing a packet of claim 5 wherein the policing results include one or more disposition recommendations, and the method further comprises the step of making a disposition decision for the packet using the policing results and at least one other disposition recommendation.

8. (original) The method of processing a packet of claim 5 further comprising the step of combining the policing results into a single result by taking a worst case policing result.

5

(9) (original) A method for policing a data packet received by a data communication switch, the method comprising:

classifying the data packet into a plurality of
10 policeable groups;

identifying policing data associated with one or
more policeable groups;

applying the policing data to produce one or more
policing results for the policeable groups; and

15 recommending a disposition of the data packet
from the policing results.

10. (original) The method of claim 9 wherein a particular policeable group identifies a type of
20 application to be policed.

11. (original) The method of claim 9 wherein the policing data includes information on bandwidth constraints specified for at least one policeable group.

25

12. (original) The method of claim 9 wherein the policing results indicate whether the data packet is to be forwarded.

30 13. (original) The method of claim 9 wherein the policing results indicate whether the data packet is eligible to be dropped.

s 339 32

14. (original) The method of claim 9 wherein the policing results indicate whether the data packet is to be dropped.

5

15. (original) The method of claim 9 wherein the step of recommending a disposition comprises the step of combining the policing results to make a recommendation.

10 16. (original) The method of claim 9 wherein the step of recommending a disposition comprises selecting one of the policing results as the recommended disposition.

15 17. (original) The method of claim 9 further comprising the step of updating the policing data based on the recommended disposition.

20 18. (original) A method for policing a data packet received by a data communication switch, the method comprising the steps of:

creating a policing database including a plurality-of-policing-data-entries-specifying-policing-data for a plurality of policeable groups;

25 applying a first identifier for retrieving a first policing data associated with a first policeable group and a second identifier identifying a second policeable group;

applying the first policing data to produce a first policing result;

30 applying the second identifier for retrieving a second policing data;

applying the second policing data to produce a second policing result; and

recommending a disposition of the data packet from the first and second policing results.

5

19. (original) The method of claim 18 wherein a particular policeable group identifies a type of application to be policed.

10 20. (original) The method of claim 18 wherein the policing data includes information on bandwidth constraints specified for the policeable group.

15 21. (original) The method of claim 18 wherein the policing results indicate whether the data packet is to be forwarded.

20 22. (original) The method of claim 18 wherein the policing results indicate whether the data packet is eligible to be dropped.

23. (original) The method of claim 18 wherein the policing results indicate whether the data packet is to be dropped.

25

24. (original) The method of claim 18 wherein the step of recommending a disposition comprises the step of combining the first and second policing results to make a recommendation.

30

25. (original) The method of claim 18 wherein the step of recommending a disposition further comprises

selecting either the first or second policing result as the recommended disposition.

26. (original) The method of claim 18 further
5 comprising the step of updating the first or second
policing data based on the recommended disposition.

10 (27). ^{π_δ'4}(original) A policing engine for a data communication node, wherein the policing engine classifies a packet into a plurality of policeable groups, and wherein the packet is compared for the respective ones of the policeable groups against respective ones of bandwidth contracts to produce respective ones of policing results.

15 (28). ^{π_δ'7}(original) A policing engine for a data communication node, wherein a first policeable group identifier is applied to a policing database to retrieve first policing data and a second policeable group identifier, wherein the first policing data is applied to produce a first policing result, and the second policeable group identifier is applied to the policing database to retrieve second policing data, wherein the second policing data is applied to produce a second policing result.

25 (29). ^{π_δ'4}(original) A packet processor comprising:
an input for receiving a packet;
policing means for classifying the packet into a plurality of policeable groups,
wherein the packet is compared against one or
30 more bandwidth contracts defined for the policeable groups to produce one or more policing results.

30. (original) The packet processor of claim 29
wherein the policing means include a policing database, a
first policeable group identifier is applied to the
policing database to retrieve first policing data and a
5 second policeable group identifier, the first policing data
is applied to produce a first policing result, the second
policeable group identifier is applied to the policing
database to retrieve second policing data, and the second
policing data is applied to produce a second policing
10 result.

31. (original) The packet processor of claim 29
further comprising a disposition means for making a
disposition decision for the packet, wherein the policing
15 results include one or more disposition recommendations,
and the disposition means use the policing results and at
least one other disposition recommendation to make the
disposition decision for the packet.

20 32. (original) The packet processor of claim 29
wherein the policing results are combined into a single
result by taking a worst-case policing result.

25 33. (new) A packet switching controller comprising:
an input for receiving a packet;
a policing element for classifying the packet
into a plurality of policeable groups,
wherein the packet is compared against one or
more bandwidths defined for the policeable groups to
30 produce one or more policing results.

Cont.

34. (new) The packet switching controller of claim 33
wherein the policing element includes a policing database,
a first policeable group identifier is applied to the
policing database to retrieve first policing data and a
5 second policeable group identifier, the first policing data
is applied to produce a first policing result, the second
policeable group identifier is applied to the policing
database to retrieve second policing data, and the second
policing data is applied to produce a second policing
10 result.

35. (new) The packet switching controller of claim 33
further comprising a disposition engine for making a
disposition decision for the packet, wherein the policing
results include one or more disposition recommendations,
15 and the disposition engine uses the policing results and at
least one other disposition recommendation to make the
disposition decision for the packet.

20 36. (new) The packet switching controller of claim 33
wherein the policing results are combined into a single
result by taking a worst case policing result.

25 ~~37.~~ (new) A method of processing a packet using a
policing element, the method comprising the steps of:
receiving the packet;
classifying the packet into a plurality of
policeable groups; and
comparing the packet against one or more
30 bandwidths defined for the policeable groups to produce one
or more policing results.

38. (new) The method of processing a packet of claim
37 wherein the policing element includes a policing
database, and the method further comprises the steps of:

5 applying a first policeable group identifier to
the policing database to retrieve first policing data and a
second policeable group identifier;

producing a first policing result using the first
policing data;

10 applying the second policeable group identifier
to the policing database to retrieve second policing data;
and

producing a second policing result using the
second policing data.

15 39. (new) The method of processing a packet of claim
37 wherein the policing results include one or more
disposition recommendations, and the method further
comprises the step of making a disposition decision for the
packet using the policing results and at least one other
20 disposition recommendation.

40. (new) The method of processing a packet of claim
37 further comprising the step of combining the policing
results into a single result by taking a worst case
25 policing result.

41. (new) A policing engine for a data communication
node, wherein the policing engine classifies a packet into
a plurality of policeable groups, and wherein the packet is
30 compared for the respective ones of the policeable groups
against respective ones of bandwidths to produce respective
ones of policing results.

Concl. 42. (new) A packet processor comprising:
an input for receiving a packet;
policing means for classifying the packet into a
plurality of policeable groups,
wherein the packet is compared against one or
more bandwidths defined for the policeable groups to
produce one or more policing results.
